(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
18. April 2002 (18.04.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/31656 A2

(51) Internationale Patentklassifikation[7]: G06F 11/00

(21) Internationales Aktenzeichen: PCT/AT01/00322

(22) Internationales Anmeldedatum:
8. Oktober 2001 (08.10.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 1723/2000 10. Oktober 2000 (10.10.2000) AT

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FTS COMPUTERTECHNIK GES.M.B.H** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: **KOPETZ, Hermann** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT). **BAUER, Günther** [AT/AT]; Dollbach 4, A-3252 Petzenkirchen (AT).

(74) Anwalt: **MATSCHNIG, Franz**; Siebensterngasse 54, A-1071 Wien (AT).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:
— *ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(54) **Title:** HANDLING ERRORS IN AN ERROR-TOLERANT DISTRIBUTED COMPUTER SYSTEM

(54) **Bezeichnung:** BEHANDELN VON FEHLERN IN EINEM FEHLERTOLERANTEN VERTEILTEN COMPUTERSYSTEM

(57) **Abstract:** The invention relates to a method for handling errors in an error-tolerant distributed computer system and such a system, with a number of nodal computers (K1...K4), connected by means of communication channels (c11...c42) with access to the channels by means of a cyclical time slice method. Messages emanating from nodal computers (K1...K4) are checked by independently formed guardians (GUA), which either convert a message suffering from an SOS (Slightly Off Specification) error into a correct message or convert the same into a message which is clearly recognisable as incorrect by all nodal computers.

(57) **Zusammenfassung:** Ein Verfahren zum Behandeln von Fehlern in einem Fehlertoleranten verteilten Computersystems, sowie ein solches System, mit einer Mehrzahl von Knotenrechnern (K1...K4), die über Kommunikationskanäle (c11...c42) verbunden sind und der Zugriff auf die Kanäle nach einem zyklischen Zeitscheibenverfahren erfolgt. Von Knotenrechnern (K1...K4) ausgehende Nachrichten werden durch unabhängig ausgebildete Guardians (GUA) überprüft, welche eine mit einem SOS ("slightly off speicification")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umformen oder in eine Nachricht, die von allen Knotenrechnern als eindeutig inkorrekt erkennbar ist.

WO 02/31656 A2

BEHANDELN VON FEHLERN IN EINEM FEHLERTOLERANTEN VERTEILTEN COMPUTERSYSTEM

Die Erfindung bezieht sich auf ein Verfahren zum Behandeln von Fehlern in einem fehlertoleranten verteilten Computersystem mit einer Mehrzahl von Knotenrechnern, die über Kommunikationskanäle verbunden sind, und jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit verfügt, wobei der Zugriff auf die Kommunikationskanäle nach einem zyklischen Zeitscheibenverfahren erfolgt und die Korrektheit von Knotenrechnern ausgehender Nachrichten durch Guardians überprüft wird.

Ebenso bezieht sich die Erfindung auf ein fehlertolerantes verteiltes Computersystem mit einer Mehrzahl von Knotenrechnern, die über zumindest eine Verteilereinheit und Kommunikationskanäle miteinander verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit verfügt, der Zugriff auf die Kommunikationskanäle nach einem zyklischen Zeitscheibenverfahren erfolgt und zur Überprüfung der von Knotenrechnern ausgehenden Nachrichten Guardians vorgesehen sind..

Sicherheitskritische technische Anwendungen, d.s. Anwendungen wo ein Fehler zu einer Katastrophe führen kann, werden zunehmend von verteilten fehlertoleranten Echtzeitcomputersystemen geführt.

In einem verteilten fehlertoleranten Echtzeitcomputersystem, bestehend aus einer Anzahl von Knotenrechnern und einem Echtzeitkommunikationssystem, soll jeder Einzelausfall eines Knotenrechners toleriert werden. Im Kern einer solchen Computerarchitektur befindet sich ein fehlertolerantes Echtzeitkommunikationssystem zum vorhersehbar schnellen und sicheren Austausch von Nachrichten.

Ein Kommunikationsprotokoll, das diese Anforderungen erfüllt, ist in der US 5,694,542 entsprechenden EP 0 658 257 beschrieben. Das Protokoll ist unter dem Namen "Time-Triggered Protokoll/C (TTP/C)" bekannt geworden und auch in Kopetz, H. (1997) *Real-Time Systems, Design Principles for Distributed Embedded Applications; ISBN: 0-7923-9894-7,* Boston, Kluwer Academic Publishers geofenbart. Es basiert auf dem bekannten zyklischen Zeitscheibenverfahren (TDMA - time-division multiple access) mit *a priori* festgelegten Zeitscheiben. TTP/C verwendet ein Verfahren zur fehlertoleranten Uhrensynchronisation, das in der US 4,866,606 geoffenbart ist.

TTP/C setzt voraus, dass das Kommunikationssystem eine logische Broadcasttopologie unterstützt und dass die Knotenrechner ein "fail-silence" Ausfallverhalten zeigen, d. h. entweder die Knotenrechner funktionieren korrekt im Wertebereich und im Zeitbereich oder sie

sind ruhig. Die Verhinderung von Fehlern im Zeitbereich, d. s., der sogenannten "Babbling Idiot" Fehler, wird in TTP/C durch eine unabhängige Fehlererkennungseinheit, dort "Bus-Guardian" genannt, erreicht, der über eine unabhängige Zeitbasis verfügt und das Zeitverhalten des Knotenrechners kontinuierlich überprüft. Um die Fehlertoleranz zu realisieren, werden mehrere fail-silent Knotenrechner zu einer fehlertoleranten Einheit (fault-tolerant unit - FTU) zusammengefasst und das Kommunikationssystem repliziert. Solange ein Knotenrechner einer FTU und ein Replikat des Kommunikationssystems funktionieren, werden die Dienste der FTU im Zeit- und Wertebereich rechtzeitig erbracht.

Eine logische Broadcasttopologie der Kommunikation kann physikalisch entweder durch ein verteiltes Bussystem, ein verteiltes Ringsystem oder durch eine zentrale Verteilereinheit (z. B. einen Sternkoppler) mit Punkt-zu-Punkt Verbindungen zu den Knotenrechnern aufgebaut werden. Wenn ein verteiltes Bussystem oder ein verteiltes Ringsystem aufgebaut wird, so muss jeder Knotenrechner über seinen eigenen BusGuardian verfügen. Wird hingegen eine zentrale Verteilereinheit verwendet, so können alle Guardians in diese Verteilereinheit integriert werden, die aufgrund der globalen Beobachtung des Verhaltens aller Knoten ein reguläres Sendeverhalten im Zeitbereich effektiv erzwingen kann. Dies ist in der nachveröffentlichten WO 01/13230 A1 beschrieben.

In einem verteilten Computersystem sind Fehler, die zu einem inkonsistenten Systemzustand führen können, besonders kritisch. Als Beispiel sei hier eine sogenannte "brake-by-wire" Applikation in einem Auto angeführt, bei welcher ein zentraler Bremscomputer Bremsnachrichten an vier Radcomputer bei den Rädern sendet. Wenn eine Bremsnachricht von zwei Radcomputern richtig empfangen wird und die beiden anderen Radcomputer die Nachricht nicht empfangen, so entsteht ein inkonsistenter Zustand. Wenn nun eine Bremsung von zwei Rädern, die auf der gleichen Seite des Fahrzeugs liegen, erfolgt, kann das Fahrzeug außer Kontrolle geraten. Die hier beschriebene Fehlerart wird in der Literatur auch als Byzantinischer Fehler (Kopetz, p. 60, p. 133) bezeichnet. Die schnelle Erkennung und richtige Behandlung von Byzantinischen Fehlern ist eines der schwierigen Probleme der Informatik.

Eine Unterklasse der Byzantinischen Fehler wird von den "Slightly-Off-Specification", kurz SOS-Fehlern gebildet. Ein SOS-Fehler kann an der Schnittstelle zwischen Analogtechnik und Digitaltechnik auftreten. Auf dem vorliegenden Fachgebiet werden unter „Digitalsignalen" logische Signale verstanden, unter „Analogsignalen" jedoch alle physikalischen Signale. In diesem Sinne ist hier auch die Unterscheidung zwischen Analog- und Digitaltechnik zu verstehen. In der Realisierung einer Datenübertragung kann jedes logische Bit auf der Leitung durch einen Signalwert (z. B. Spannung aus einem spezifizierten Spannungstoleranzintervall) während eines spezifizierten Zeitintervalls dargestellt werden. Ein korrekter Sender

muss seine Analogsignale innerhalb der spezifizierten Toleranzintervalle generieren, damit sichergestellt ist, dass alle korrekten Empfänger diese Signale auch korrekt interpretieren. Wenn nun ein Sender einer Nachricht ein Signal knapp (Slightly-Off-Specification) außerhalb des spezifizierten Intervalls (im Wertebereich, im Zeitbereich, oder in beiden) generiert, so kann der Fall eintreten, dass einige Empfänger dieses Signal richtig interpretieren, während andere Empfänger das Signal nicht richtig interpretieren können. Wir bezeichnen eine solche Broadcastnachricht als *SOS-falsch*. In der Folge kann ein Byzantinischer Fehler, wie oben anhand eines Bremssystems beschrieben, auftreten. Ein solcher Fehler kann seine Ursache in einer fehlerhaften Spannungsversorgung, einem fehlerhaften Taktgeber oder einem durch Alterung geschwächten Bauteil haben. Die Übertragung einer Nachricht auf zwei Kommunikationskanälen kann SOS-Fehler nicht verhindern, wenn die Fehlerursache, z. B. ein fehlerhafter Taktgeber des Rechnerknotens, der die Bitfolge generiert, beide Kanäle betrifft.

Es ist ein Grundsatz der Sicherheitstechnik, auftretende Fehler zum frühestmöglichen Zeitpunkt zu erkennen, um Gegenmaßnahmen ergreifen zu können, ehe Folgefehler weiteren Schaden anrichten. Diesem Grundsatz wird im zitierten TTP/C Protokoll (EP 0 658 257) dadurch entsprochen, dass SOS-Fehler über den sogenannten Membershipalgorithmus des TTP/C Protokolls innerhalb von maximal zwei TDMA-Runden konsistent erkannt werden. Da es sich bei SOS-Fehlern typischerweise um sehr selten auftretende transiente Fehler handelt, werden in einer bestehenden Prototypimplementierung von TTP/C SOS-Fehler der auch sehr selten auftretenden Klasse der nahe-koinzidenten Mehrfachfehler zugewiesen und wie diese behandelt.

Eine Aufgabe der Erfindung liegt darin, ein Tolerieren von Fehlern der SOS-Klasse in einem verteilten Computersystem durch geeignete Maßnahmen zu ermöglichen.

Diese Aufgabe wird mit einem Verfahren der eingangs genannten Art gelöst, bei welchen erfindungsgemäß die unabhängig ausgebildeten Guardians eine mit einem SOS („slightly off specifications")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umformen oder in eine Nachricht die von allen empfangenden Knotenrechnern als eindeutig inkorrekt erkennbar ist.

Die Aufgabe wird auch mit einem fehlertoleranten verteilten Computersystem der oben angegebenen Art gelöst, bei welchem erfindungsgemäß die unabhängig ausgebildeten Guardians dazu eingerichtet sind, eine mit einem SOS („Slightly off specifications")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umzuformen oder in eine Nachricht, die von allen empfangenden Knotenrechnern als eindeutig inkorrekt erkennbar ist.

Dank der Erfindung kann in einer zeitgesteuerten, verteilten, fehlertoleranten Architektur für hochzuverlässige Echtzeit-Computeranwendungen auch die Fehlerklasse der „slightly off specification" (SOS)-Fehler toleriert werden.

Bei einer vorteilhaften Variante ist vorgesehen, dass jeder unabhängige Guardian unter Stützung auf seine unabhängige Zeitbasis überprüft, ob der Beginn einer von der Kommunikationskontrolleinheit eines Knotenrechners gesendeten Nachricht innerhalb des dem Guardian a priori bekannten Beginnzeitfensters der Nachricht fällt, und der den entsprechenden Kommunikationskanal sofort schließt, falls die Nachricht außerhalb dieses Zeitfensters liegt, damit eine unvollständige, von allen empfangenden Knotenrechnern als inkorrekt erkennbare Nachricht entsteht. Auf diese Weise lässt sich das Auftreten von nur leicht verstümmelten, möglicherweise von den Empfängern fälschlicherweise als korrekt interpretierten Nachrichten verhindern.

Zweckmäßig ist es weiters, wenn ein Guardian das eingehende physikalische Signal jeder Nachricht im Zeit- und Wertebereich unter Berücksichtigung der relevanten Codierungsvorschriften und unter Verwendung seiner lokalen Zeitbasis und seiner lokalen Stromversorgung regeneriert. Ein solches unabhängiges Regenerieren erhöht die geforderte Sicherheit des Systems wesentlich.

Eine andere vorteilhafte Weiterbildung der Erfindung sieht vor, dass ein keine Nachrichten empfangender Guardian keine Nachrichten mit korrekter CRC und korrekter Länge generiert. Auch diese Maßnahme kann die Sicherheit des Systems weiter steigern.

Eine optimale Steuerung auf Basis des Beginnzeitfensters sieht vor, dass das Beginnzeitfenster eines Guardians um mehr als die Präzision des Systems nach dem Beginnzeitfenster eines Knotenrechners beginnt und das Beginnzeitenfenster eines Guardians um mehr als die Präzision vor dem Beginnzeitfenster eines Knotenrechners endet.

Zusätzliche Vorteile nicht nur hinsichtlich der Sicherheit sondern auch in Bezug auf die Realisierungskosten des Systems ergeben sich, falls die Guardians in die zumindest eine Verteilereinheit integriert sind, und die Verteilereinheit über eine unabhängige Stromversorgung und über eine unabhängige, fehlertolerante verteilte Uhrensynchronisation verfügt.

Die Erfindung samt weiterer Vorteile ist im folgenden anhand von Ausführungsbeispielen näher erläutert, die in der Zeichnung veranschaulicht sind. In dieser zeigen

Fig. 1 schematisch ein verteiltes Computersystem, bestehend aus vier Knotenrechnern, die über zwei replizierte zentrale Verteilereinheiten miteinander verbunden sind,

Fig. 2 eine Fault Containment Unit, gebildet aus einem Knotenrechner und zwei Guardians und

Fig. 3 die Lage der Beginnzeitfenster eines Guardians und eines Knotenrechners.

Fig. 1 zeigt ein System von vier Knotenrechnern K1, K2, K3, K4, wobei jeder Knotenrechner eine austauschbare Einheit bildet und mit je einer Punkt-zu-Punkt Verbindung oder Kommunikationskanal c11 ... c42 mit einer von zwei replizierten zentralen Verteilereinheiten V1 oder V2 verbunden ist. Zwischen jedem Ausgang eines Knotenrechners und jedem Eingang der Verteilereinheit befindet sich ein Guardian GUA, der entweder selbständig ausgeführt ist oder in die Verteilereinheit integriert werden kann. Die prinzipielle Funktion eines Guardian oder BusGuardian ist in Kopetz, p. 173 erläutert. Um seine Funktion erfüllen zu können, benötigt ein Guardian neben einem Controller auch Schalter um Kanäle zu öffnen bzw. zu sperren. Zwei unidirektionale Kommunikationskanäle v21, v12 zwischen den Verteilereinheiten V1 und V2 dienen der wechselseitigen Überwachung und dem Informationsaustausch der zentralen Verteilereinheiten V1 und V2. Wie gleichfalls aus Kopetz, z. B. p. 172 - 177, hervorgeht, besitzt jeder Knotenrechner K1 ... K4 einen autonomen Controller CON oder Kommunikationscontroller, der mit den replizierten Kommunikationskanälen, z. B. c11, c12 verbunden ist. Angedeutete Verbindungen w1, w2 sind dedizierte Kommunikationskanäle. Sie führen zu Wartungscomputern w1, w2, welche die Parameter der Verteilereinheiten und deren korrekte Funktionen überwachen können.

Fig. 2 zeigt einen Knotenrechner K1 mit seinem Kommunikationscontroller CON und den Kommunikationskanälen c11, c21 zu den anderen Knotenrechnern bzw. Verteilereinheiten des verteilten Computersystems. Hier sind die Guardians GUA als BusGuardians für die Kommunikationskanäle c11, c21 vorgesehen, doch können sie gemäß Fig. 1 in die beiden unabhängigen zentralen Verteilereinheiten V1, V2 integriert sein. Logisch gesehen bilden die drei Subsysteme Knotenrechner + zwei Guardians eine Einheit, die hier „Fault Containment Unit" FCU bezeichnet wird und so in Fig. 2 angeschrieben ist; dies wie gesagt unabhängig davon, ob die Guardians GUA physikalisch in die zentralen Verteilereinheiten oder in die Knotenrechner integriert sind.

Nun sei auf Fig. 3 Bezug genommen, in welcher Beginnzeitfenster für den Anfang einer Nachricht eingetragen sind. Man unterscheidet zwischen dem Beginnfenster T_{CON} mit eben dieser Länge T_{CON} eines Knotenrechners bzw. seines Controllers und dem Beginnzeitfenster

T_{GUA} eines Guardians. Die Erfindung sieht vor, dass das Zeitfenster T_{GUA} eines Guardians kürzer als das Zeitfenster T_{CON} eines Knotenrechners ist und zwischen dem in das Fenster T_{CON} eingebetteten Zeitfenster T_{GUA} ein Abstand $\tau 1$ bzw. $\tau 2$ verbleibt, der größer als die Präzision P des Systems ist. Der Begriff der Präzision ist z. B. in Kopetz, Kapitel 3.1.3 „Precision and Accurancy", p. 49 und 50 erläutert.

Wir bezeichnen nun einen beliebigen Fehler eines aktiven Subsystems, z. B. des Knotenrechners K1, als *beliebig aktiv* (unconstrained active). Wir bezeichnen weiters einen Fehler eines passiven Subsystems, z. B. eines Guardians oder einer Verbindung c11 oder c22 als *beliebig passiv* (unconstrained passiv), wenn durch die Konstruktion des passiven Subsystems sichergestellt ist, dass dieses Subsystem aus sich heraus, d. h. ohne eine Eingabe von einem aktiven Subsystem, keine Bitfolge generieren kann, die von einem Empfänger als syntaktisch richtige Nachricht interpretiert werden kann. Eine Nachricht ist *syntaktisch richtig*, wenn eine CRC Überprüfung keinen Fehler anzeigt, sie die erwartete richtige Länge hat, den Codierungsvorschriften entspricht und innerhalb des erwarteten Zeitintervalls eintrifft.

Wenn ein passives Subsystem nicht über das Wissen verfügt, wie ein korrektes CRC zu generieren ist (hat keinen Zugriff auf den CRC Generierungsalgorithmus) und wie lange eine korrekte Nachricht sein muss, so ist die Wahrscheinlichkeit, dass aufgrund von statistischen Zufallsprozessen (Störungen) eine syntaktisch richtige Nachricht entsteht, vernachlässigbar klein.

Eine Fault Containment Unit FCU kann einen beliebigen aktiven Fehler eines Knotenrechners K1 oder einen beliebigen passiven Fehler eines der beiden Guardians GUA in einen Fehler, der kein byzantinischer Fehler ist, umwandeln, wenn folgende Annahmen erfüllt werden:

(i) ein korrekter Knotenrechner K1 sendet auf beiden Kanälen c11 und c12 die gleiche syntaktisch richtige Nachricht und

(ii) ein korrekter Guardian GUA formt eine SOS-falsche Nachricht von dem Knotenrechner K1 entweder in eine syntaktisch richtige Nachricht oder in eine Nachricht um, die von allen Empfängern als eindeutig inkorrekt erkannt werden kann (nicht SOS Nachricht) und

(iii) während des Sendens einer Nachricht ist maximal eines der angeführten Subsysteme fehlerhaft.

Aufgrund der Fehlerannahme (iii) kann nur ein einziges der drei angeführten Subsysteme K1, GUA, GUA fehlerhaft sein. Ist der Knotenrechner K1 beliebig fehlerhaft, so sind die

beiden Guardians GUA und GUA nicht fehlerhaft und generieren entsprechend Annahme (ii) nicht-SOS Nachrichten. Ist einer der beiden Guardians GUA beliebig passiv fehlerhaft, so generiert der Knotenrechner K1 eine syntaktisch richtige Nachricht und überträgt diese syntaktisch richtige Nachricht an beide Guardians GUA (Annahme i). Der korrekte Guardian GUA überträgt nun die Nachricht korrekt an alle Empfänger, d. h. Knotenrechner. Aufgrund der Empfangslogik und dem Selbstvertrauensprinzip des TTP/C-Protokolls werden in diesem Fall alle richtigen Empfänger die richtige Nachricht auswählen und den sendenden Knotenrechner als richtig klassifizieren. Um SOS-Fehler zu tolerieren, ist keine Änderung im TTP/C-Protokoll erforderlich.

Eine beliebige Nachricht kann aus folgenden drei Gründen SOS-falsch sein:

(i) die Nachricht hat einen SOS-Fehler im Wertebereich und/oder

(ii) die Nachricht hat einen inneren SOS Fehler im Zeitbereich (z. B., Timing Fehler innerhalb des Codes) und/oder

(iii) die Übertragung der Nachricht wird knapp außerhalb des spezifizierten Sendeintervalls (siehe Fig. 3) begonnen.

Ein korrekter Guardian (GUA) verwandelt diese Fehlerursachen wie folgt in nicht SOS-Fehler:

(i) Die Ausgabewerte der Nachricht werden durch eine Guardian GUA mit der unabhängigen Spannungsversorgung des Guardians regeneriert.

(ii) Die Codierung der Nachricht wird durch einen Guardian GUA mit der unabhängigen Zeitbasis des BusGuardian regeneriert.

(iii) Der Guardian sperrt den Kanal, sobald er erkennt, dass die Übertragung außerhalb des spezifizierten Zeitintervalls T_{GUA} begonnen hat. Damit erhalten alle Empfänger, d. h. Knotenrechner stark verstümmelte Nachrichten, die als fehlerhaft erkannt werden.

Ein Sperren des Kanals durch einen Guardian GUA unmittelbar nach dem spezifizierten Ende der Übertragungszeit einer Nachricht ist im allgemeinen nicht ausreichend, um SOS-Fehler zu verhindern, da nicht auszuschließen ist, dass eine durch das Sperren schwach verstümmelte Nachricht Anlass für einen SOS-Fehler eines an sich fehlerfreien Guardians GUA sein kann. Wenn nun beide Guardians die Nachricht in der gleichen Weise schwach verstümmeln, so kann ein SOS-Fehler auf Systemebene entstehen.

Abschließend sei festgehalten, dass sich diese Erfindung nicht auf die beschriebene Realisierung mit vier Knotenrechnern beschränkt, sondern beliebig erweiterbar ist. Sie ist nicht nur beim TTP/C Protokoll, sondern auch bei anderen zeitgesteuerten Protokollen anwendbar.

PATENTANSPRÜCHE

1. Verfahren zum Behandeln von Fehlern in einem fehlertoleranten verteilten Computersystem mit einer Mehrzahl von Knotenrechnern (K1 ... K4), die über Kommunikationskanäle (c11 ... c42) verbunden sind, und jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit (CON) verfügt, wobei der Zugriff auf die Kommunikationskanäle nach einem zyklischen Zeitscheibenverfahren erfolgt und die Korrektheit von Knotenrechnern ausgehender Nachrichten durch Guardians (GUA) überprüft wird und

   dadurch gekennzeichnet, dass

   die unabhängig ausgebildeten Guardins (GUA) eine mit einem SOS („slightly off specifications")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umformen oder in eine Nachricht die von allen empfangenden Knotenrechnern (K1 ... K4) als eindeutig inkorrekt erkennbar ist.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet, dass** jeder unabhängige Guardian (GUA) unter Stützung auf seine unabhängige Zeitbasis überprüft, ob der Beginn einer von der Kommunikationskontrolleinheit (CON) eines Knotenrechners (K1 ... K4) gesendeten Nachricht innerhalb des dem Guardian (GUA) a priori bekannten Beginnzeitfensters (T_{GUA}) der Nachricht fällt, und der den entsprechenden Kommunikationskanal (c11 ... c42) sofort schließt, falls die Nachricht außerhalb dieses Zeitfensters liegt, damit eine unvollständige, von allen empfangenden Knotenrechnern als inkorrekt erkennbare Nachricht entsteht.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet, dass** ein Guardian (GUA) das eingehende physikalische Signal jeder Nachricht im Zeit- und Wertebereich unter Berücksichtigung der relevanten Codierungsvorschriften und unter Verwendung seiner lokalen Zeitbasis und seiner lokalen Stromversorgung regeneriert.

4. Verfahren nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** ein keine Nachrichten empfangender Guardian (GUA) keine Nachrichten mit korrekter CRC und korrekter Länge generiert.

5. Verfahren nach einem der Ansprüche 2 bis 4, **dadurch gekennzeichnet, dass** das Beginnzeitfenster (T_{GUA}) eines Guardians (GUA) um mehr als die Präzision (P) des Systems nach dem Beginnzeitfenster (T_{CON}) eines Kostenrechners (K1 ... K4) beginnt und

das Beginnzeitenfenster eines Guardians um mehr als die Präzision vor dem Beginnzeitfenster eines Knotenrechners endet.

6. Fehlertolerantes verteiltes Computersystem mit einer Mehrzahl von Knotenrechnern (K1 ... K4), die über zumindest eine Verteilereinheit (V1, V2) und Kommunikationskanäle (c11 ... c42) miteinander verbunden sind, jeder Knotenrechner über eine autonome Kommunikationskontrolleinheit (CON) verfügt, der Zugriff auf die Kommunikationskanäle nach einem zyklischen Zeitscheibenverfahren erfolgt und zur Überprüfung der von Knotenrechnern ausgehenden Nachrichten Guardians (GUA) vorgesehen sind,

dadurch gekennzeichnet, dass

die unabhängig ausgebildeten Guardians (GUA) dazu eingerichtet sind, eine mit einem SOS („Slightly off specifications")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umzuformen oder in eine Nachricht, die von allen empfangenden Knotenrechnern (K1 ... K4) als eindeutig inkorrekt erkennbar ist.

7. Computersystem nach Anspruch 6, **dadurch gekennzeichnet, dass** ein Guardian (GUA) eine unabhängige Zeitbasis besitzt und dazu eingerichtet ist, zu überprüfen, ob der Beginn einer von der Kommunikationskontrolleinheit (CON) eines Knotenrechners (K1 ... K4) gesendeten Nachricht innerhalb des dem Guardian (GUA) a priori bekannten Beginnzeitfensters (T_{GUA}) der Nachricht fällt, sowie dazu, den entsprechenden Kommunikationskanal (c11 ... c42) sofort zu schließen, falls die Nachricht außerhalb dieses Zeitfensters liegt, damit eine unvollständige, von allen empfangenden Knotenrechnern als inkorrekt erkennbare Nachricht entsteht.

8. Computersystem nach Anspruch 5 oder 6, **dadurch gekennzeichnet, dass** ein Guardian (GUA) dazu eingerichtet ist, das eingehende physikalische Signal jeder Nachricht im Zeit- und Wertebereich unter Berücksichtigung der relevanten Codierungsvorschriften und unter Verwendung seiner lokalen Zeitbasis und seiner lokalen Stromversorgung zu regenerieren.

9. Computersystem nach einem der Ansprüche 6 bis 8, **dadurch gekennzeichnet, dass** ein Guardian (GUA) dazu eingerichtet ist, falls er keine Nachricht empfängt, auch keine Nachrichten mit korrekter CRC und korrekter Länge zu generieren.

10. Computersystem nach einem der Ansprüche 6 bis 9, **dadurch gekennzeichnet, dass** der Anfang des Beginnzeitfensters (T_{CON}) eines Knotenrechners (K1 ... K4) um mehr

als die Präzision (P) des Systems vor dem Anfang des Beginnzeitfensters (T_{GUA}) eines Guardians (GUA) liegt und das Ende des Beginnzeitfensters eines Guardians um mehr als die Präzision vor dem Ende des Beginnzeitfensters eines Kostenrechners liegt.

11. Computersystem nach einem der Ansprüche 6 bis 10, **dadurch gekennzeichnet, dass** die Guardians (GUA) in die zumindest eine Verteilereinheit (V1, V2) integriert sind, und die Verteilereinheit über eine unabhängige Stromversorgung und über eine unabhängige, fehlertolerante verteilte Uhrensynchronisation verfügt.

1/1

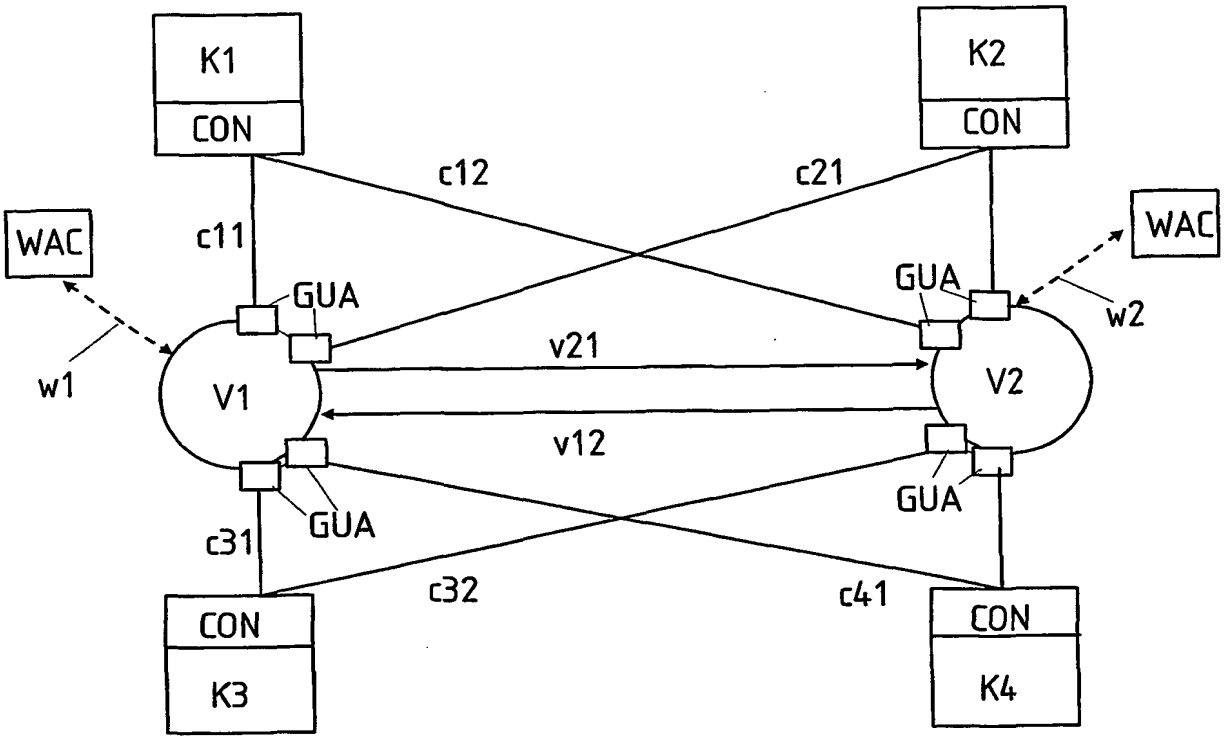


Fig. 1

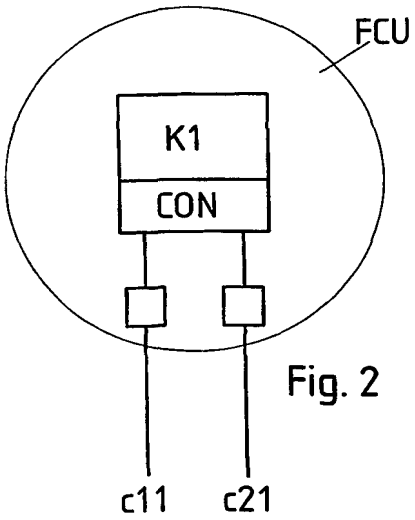


Fig. 2

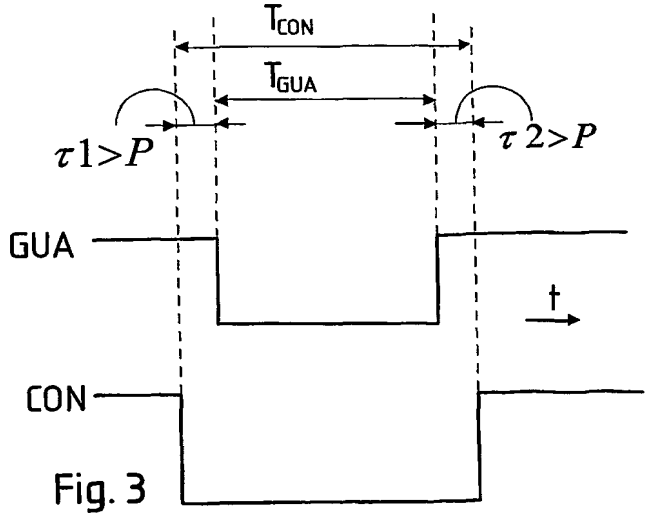


Fig. 3

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
18. April 2002 (18.04.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/031656 A3

(51) Internationale Patentklassifikation[7]: G06F 11/00, 13/372

(21) Internationales Aktenzeichen: PCT/AT01/00322

(22) Internationales Anmeldedatum:
8. Oktober 2001 (08.10.2001)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
A 1723/2000 10. Oktober 2000 (10.10.2000) AT

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **FTS COMPUTERTECHNIK GES.M.B.H** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **KOPETZ, Hermann** [AT/AT]; Föhrenweg 8, A-2500 Baden-Siegenfeld (AT). **BAUER, Günther** [AT/AT]; Dollbach 4, A-3252 Petzenkirchen (AT).

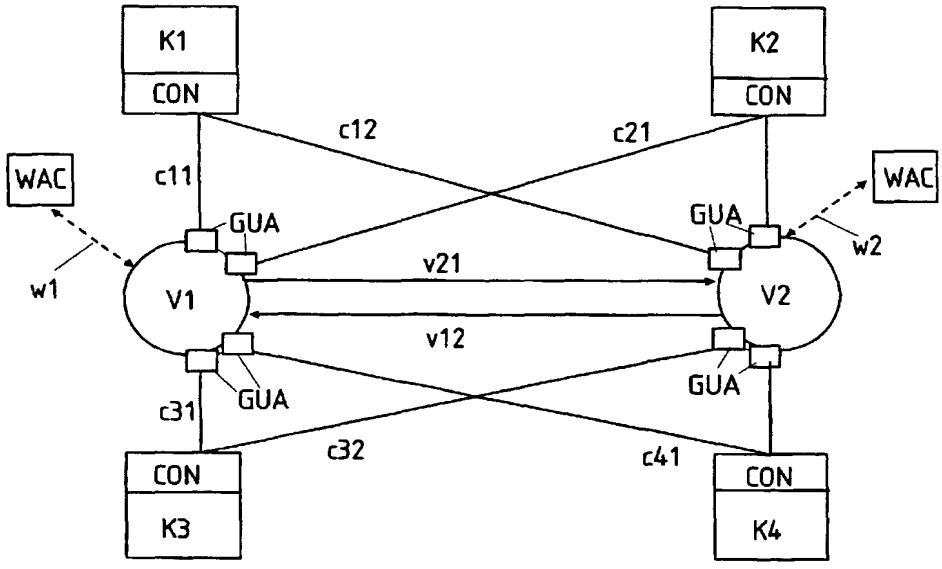
(74) Anwalt: **MATSCHNIG, Franz**; Siebensterngasse 54, A-1071 Wien (AT).

(81) Bestimmungsstaaten *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

[Fortsetzung auf der nächsten Seite]

(54) Title: HANDLING ERRORS IN AN ERROR-TOLERANT DISTRIBUTED COMPUTER SYSTEM

(54) Bezeichnung: BEHANDELN VON FEHLERN IN EINEM FEHLERTOLERANTEN VERTEILTEN COMPUTERSYSTEM



(57) Abstract: The invention relates to a method for handling errors in an error-tolerant distributed computer system and such a system, with a number of nodal computers (K1...K4), connected by means of communication channels (c11...c42) with access to the channels by means of a cyclical time slice method. Messages emanating from nodal computers (K1...K4) are checked by independently formed guardians (GUA), which either convert a message suffering from an SOS (Slightly Off Specification) error into a correct message or convert the same into a message which is clearly recognisable as incorrect by all nodal computers.

[Fortsetzung auf der nächsten Seite]

WO 02/031656 A3

(84) Bestimmungsstaaten *(regional)*: ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— *mit internationalem Recherchenbericht*

— *vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen*

(88) Veröffentlichungsdatum des internationalen Recherchenberichts: 25. Juli 2002

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Ein Verfahren zum Behandeln von Fehlern in einem Fehlertoleranten verteilten Computersystems, sowie ein solches System, mit einer Mehrzahl von Knotenrechnern (K1...K4), die über Kommunikationskanäle (c11...c42) verbunden sind und der Zugriff auf die Kanäle nach einem zyklischen Zeitscheibenverfahren erfolgt. Von Knotenrechnern (K1...K4) ausgehende Nachrichten werden durch unabhängig ausgebildete Guardians (GUA) überprüft, welche eine mit einem SOS ("slightly off speicification")-Fehler behaftete Nachricht entweder in eine korrekte Nachricht umformen oder in eine Nachricht, die von allen Knotenrechnern als eindeutig inkorrekt erkennbar ist.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/AT 01/00322

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/00 G06F13/372

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KOPETZ H. ET AL: "Tolerating Arbitrary Node Failures in the Time-Triggered Architecture" REAL-TIME SYSTEMS GROUP - PAPER SERVER, 'Online! March 2001 (2001-03), pages 1-7, XP002196878 Retrieved from the Internet: <URL:http://www.vmars.tuwien.ac.at/frame-papers.html> 'retrieved on 2002-04-22!	1,6,11
Y	the whole document	2,7
A	--- -/--	3-5,8-10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 April 2002	22/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Leuridan, K

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KOPETZ H ET AL: "The transparent implementation of fault tolerance in the time-triggered architecture" DEPENDABLE COMPUTING FOR CRITICAL APPLICATIONS 7, 1999 SAN JOSE, CA, USA 6-8 JAN. 1999, PISCATAWAY, NJ, USA,IEEE, US, 6 January 1999 (1999-01-06), pages 191-205, XP010366438 ISBN: 0-7695-0284-9 the whole document	1,6
A	---	2-5,7-10
Y	EP 0 622 712 A (ALLEN BRADLEY CO) 2 November 1994 (1994-11-02) column 8, line 17 -column 11, line 1 column 30, line 10 -column 33, line 31 figure 3	2,7
A	--- KOPETZ H ET AL: "TEMPORAL UNCERTAINTIES IN INTERACTIONS AMONG REAL-TIME OBJECTS" PROCEEDINGS OF THE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS. HUNTSVILLE, OCT. 9 - 11, 1990, LOS ALAMITOS. IEEE COMP. SOC. PRESS, US, vol. SYMP. 9, 9 October 1990 (1990-10-09), pages 165-174, XP000278470 ISBN: 0-8186-2081-1 the whole document	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/AT 01/00322

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0622712 A	02-11-1994	US 5537549 A	16-07-1996
		EP 0622712 A2	02-11-1994

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen	PCT/AT 01/00322

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/00 G06F13/372

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06F H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, INSPEC, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	KOPETZ H. ET AL: "Tolerating Arbitrary Node Failures in the Time-Triggered Architecture" REAL-TIME SYSTEMS GROUP - PAPER SERVER, 'Online! März 2001 (2001-03), Seiten 1-7, XP002196878 Gefunden im Internet: <URL:http://www.vmars.tuwien.ac.at/frame-papers.html> 'gefunden am 2002-04-22!	1,6,11
Y	das ganze Dokument	2,7
A		3-5,8-10
	--- -/--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
22. April 2002	22/05/2002

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Leuridan, K

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/AT 01/00322

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	KOPETZ H ET AL: "The transparent implementation of fault tolerance in the time-triggered architecture" DEPENDABLE COMPUTING FOR CRITICAL APPLICATIONS 7, 1999 SAN JOSE, CA, USA 6-8 JAN. 1999, PISCATAWAY, NJ, USA,IEEE, US, 6. Januar 1999 (1999-01-06), Seiten 191-205, XP010366438 ISBN: 0-7695-0284-9 das ganze Dokument	1,6
A		2-5,7-10
Y	EP 0 622 712 A (ALLEN BRADLEY CO) 2. November 1994 (1994-11-02) Spalte 8, Zeile 17 -Spalte 11, Zeile 1 Spalte 30, Zeile 10 -Spalte 33, Zeile 31 Abbildung 3	2,7
A	KOPETZ H ET AL: "TEMPORAL UNCERTAINTIES IN INTERACTIONS AMONG REAL-TIME OBJECTS" PROCEEDINGS OF THE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS. HUNTSVILLE, OCT. 9 - 11, 1990, LOS ALAMITOS. IEEE COMP. SOC. PRESS, US, Bd. SYMP. 9, 9. Oktober 1990 (1990-10-09), Seiten 165-174, XP000278470 ISBN: 0-8186-2081-1 das ganze Dokument	1-11

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

ationales Aktenzeichen
PCT/AT 01/00322

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0622712 A	02-11-1994	US 5537549 A	16-07-1996
		EP 0622712 A2	02-11-1994

DOCKET NO: P2002,0542
SERIAL NO:
APPLICANT: Charles Seeley et al.

LERNER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100